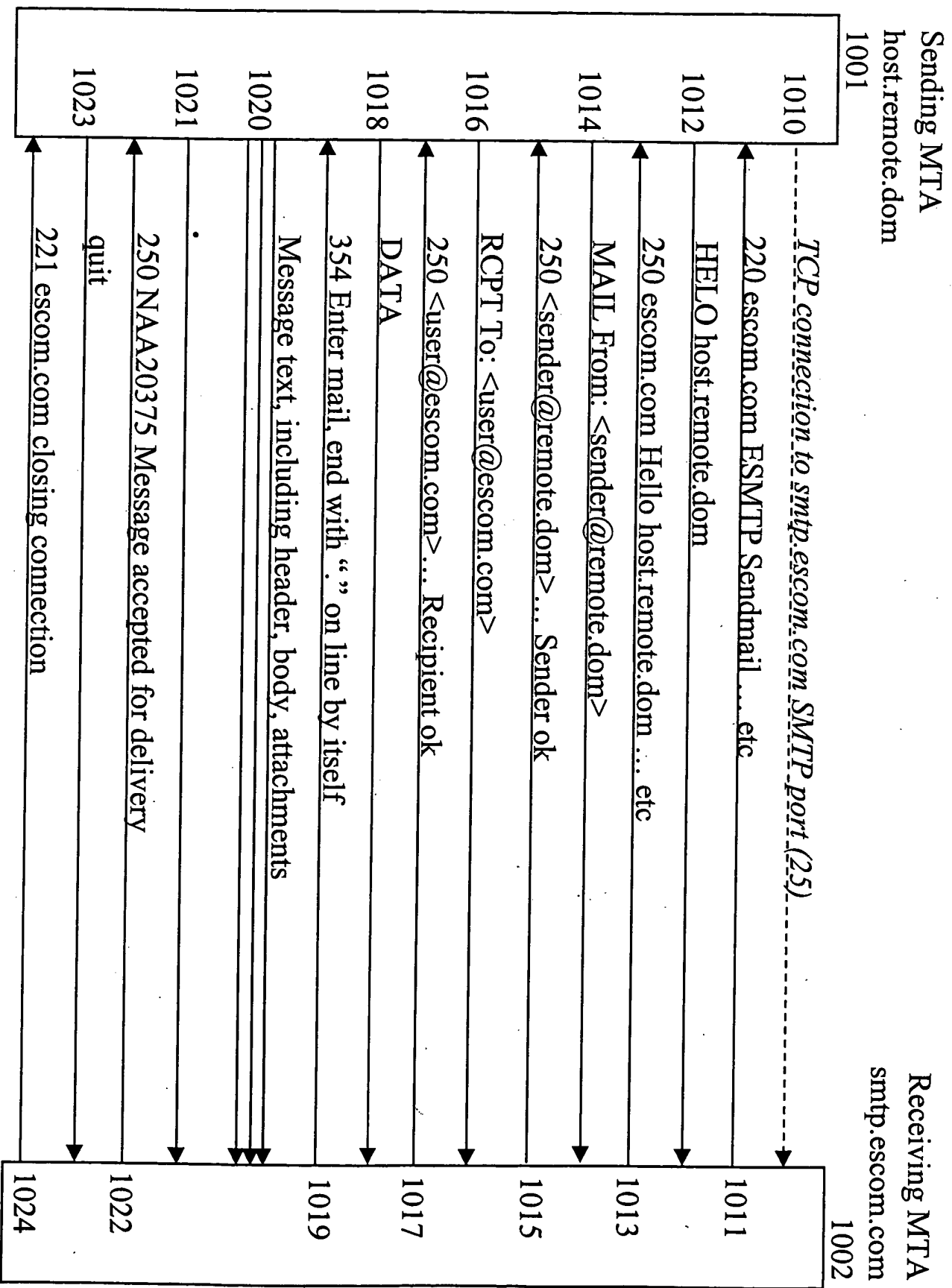




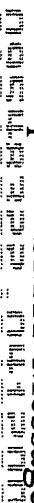
Figure 1. SMTP Architecture

GROUP	1944-45	1945-46	1946-47	1947-48	1948-49	1949-50	1950-51	1951-52	1952-53	1953-54	1954-55	1955-56	1956-57	1957-58	1958-59	1959-60	1960-61	1961-62	1962-63	1963-64	1964-65	1965-66	1966-67	1967-68	1968-69	1969-70	1970-71	1971-72	1972-73	1973-74	1974-75	1975-76	1976-77	1977-78	1978-79	1979-80	1980-81	1981-82	1982-83	1983-84	1984-85	1985-86	1986-87	1987-88	1988-89	1989-90	1990-91	1991-92	1992-93	1993-94	1994-95	1995-96	1996-97	1997-98	1998-99	1999-00	2000-01	2001-02	2002-03	2003-04	2004-05	2005-06	2006-07	2007-08	2008-09	2009-10	2010-11	2011-12	2012-13	2013-14	2014-15	2015-16	2016-17	2017-18	2018-19	2019-20	2020-21	2021-22	2022-23	2023-24	2024-25	2025-26	2026-27	2027-28	2028-29	2029-30	2030-31	2031-32	2032-33	2033-34	2034-35	2035-36	2036-37	2037-38	2038-39	2039-40	2040-41	2041-42	2042-43	2043-44	2044-45	2045-46	2046-47	2047-48	2048-49	2049-50	2050-51	2051-52	2052-53	2053-54	2054-55	2055-56	2056-57	2057-58	2058-59	2059-60	2060-61	2061-62	2062-63	2063-64	2064-65	2065-66	2066-67	2067-68	2068-69	2069-70	2070-71	2071-72	2072-73	2073-74	2074-75	2075-76	2076-77	2077-78	2078-79	2079-80	2080-81	2081-82	2082-83	2083-84	2084-85	2085-86	2086-87	2087-88	2088-89	2089-90	2090-91	2091-92	2092-93	2093-94	2094-95	2095-96	2096-97	2097-98	2098-99	2099-00	2100-01	2101-02	2102-03	2103-04	2104-05	2105-06	2106-07	2107-08	2108-09	2109-10	2110-11	2111-12	2112-13	2113-14	2114-15	2115-16	2116-17	2117-18	2118-19	2119-20	2120-21	2121-22	2122-23	2123-24	2124-25	2125-26	2126-27	2127-28	2128-29	2129-30	2130-31	2131-32	2132-33	2133-34	2134-35	2135-36	2136-37	2137-38	2138-39	2139-40	2140-41	2141-42	2142-43	2143-44	2144-45	2145-46	2146-47	2147-48	2148-49	2149-50	2150-51	2151-52	2152-53	2153-54	2154-55	2155-56	2156-57	2157-58	2158-59	2159-60	2160-61	2161-62	2162-63	2163-64	2164-65	2165-66	2166-67	2167-68	2168-69	2169-70	2170-71	2171-72	2172-73	2173-74	2174-75	2175-76	2176-77	2177-78	2178-79	2179-80	2180-81	2181-82	2182-83	2183-84	2184-85	2185-86	2186-87	2187-88	2188-89	2189-90	2190-91	2191-92	2192-93	2193-94	2194-95	2195-96	2196-97	2197-98	2198-99	2199-00	2200-01	2201-02	2202-03	2203-04	2204-05	2205-06	2206-07	2207-08	2208-09	2209-10	2210-11	2211-12	2212-13	2213-14	2214-15	2215-16	2216-17	2217-18	2218-19	2219-20	2220-21	2221-22	2222-23	2223-24	2224-25	2225-26	2226-27	2227-28	2228-29	2229-30	2230-31	2231-32	2232-33	2233-34	2234-35	2235-36	2236-37	2237-38	2238-39	2239-40	2240-41	2241-42	2242-43	2243-44	2244-45	2245-46	2246-47	2247-48	2248-49	2249-50	2250-51	2251-52	2252-53	2253-54	2254-55	2255-56	2256-57	2257-5
-------	---------	---------	---------	---------	---------	---------	---------	---------	---------	---------	---------	---------	---------	---------	---------	---------	---------	---------	---------	---------	---------	---------	---------	---------	---------	---------	---------	---------	---------	---------	---------	---------	---------	---------	---------	---------	---------	---------	---------	---------	---------	---------	---------	---------	---------	---------	---------	---------	---------	---------	---------	---------	---------	---------	---------	---------	---------	---------	---------	---------	---------	---------	---------	---------	---------	---------	---------	---------	---------	---------	---------	---------	---------	---------	---------	---------	---------	---------	---------	---------	---------	---------	---------	---------	---------	---------	---------	---------	---------	---------	---------	---------	---------	---------	---------	---------	---------	---------	---------	---------	---------	---------	---------	---------	---------	---------	---------	---------	---------	---------	---------	---------	---------	---------	---------	---------	---------	---------	---------	---------	---------	---------	---------	---------	---------	---------	---------	---------	---------	---------	---------	---------	---------	---------	---------	---------	---------	---------	---------	---------	---------	---------	---------	---------	---------	---------	---------	---------	---------	---------	---------	---------	---------	---------	---------	---------	---------	---------	---------	---------	---------	---------	---------	---------	---------	---------	---------	---------	---------	---------	---------	---------	---------	---------	---------	---------	---------	---------	---------	---------	---------	---------	---------	---------	---------	---------	---------	---------	---------	---------	---------	---------	---------	---------	---------	---------	---------	---------	---------	---------	---------	---------	---------	---------	---------	---------	---------	---------	---------	---------	---------	---------	---------	---------	---------	---------	---------	---------	---------	---------	---------	---------	---------	---------	---------	---------	---------	---------	---------	---------	---------	---------	---------	---------	---------	---------	---------	---------	---------	---------	---------	---------	---------	---------	---------	---------	---------	---------	---------	---------	---------	---------	---------	---------	---------	---------	---------	---------	---------	---------	---------	---------	---------	---------	---------	---------	---------	---------	---------	---------	---------	---------	---------	---------	---------	---------	---------	---------	---------	---------	---------	---------	---------	---------	---------	---------	---------	---------	---------	---------	---------	---------	---------	---------	---------	---------	---------	---------	---------	---------	---------	---------	---------	---------	---------	---------	---------	---------	---------	---------	---------	---------	---------	--------



Prior Art

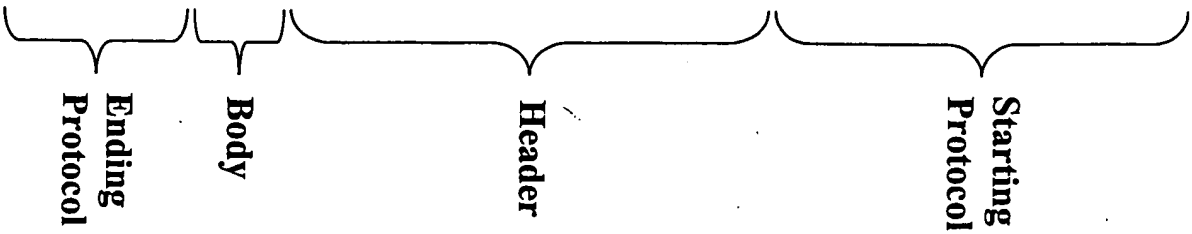
Figure 2. Example of SMTP Message Transfer



```

< 220 escom.com ESMTP Sendmail 8.9.3/8.9.3; Mon, 6 Sep 1999 21:12:35 -0400 (EDT)
> HELLO host.remote.dom
< 250 escom.com Hello host.remote.dom [192.168.255.255], pleased to meet you
> MAIL From: <sender@remote.dom>
< 250 <sender@remote.dom>... Sender ok
> RCPT To: <user@escom.com>
< 250 <user@escom.com>... Recipient ok
> DATA
< 354 Enter mail, end with "." on a line by itself
> Received: from remote.dom (host.remote.dom [192.168.255.255])
>   by smtp.escom.com (8.9.3/8.9.3) with ESMTP id NAA20375
>   for <user@escom.com>; Mon, 6 Sep 1999 21:12:39 -0400 (EDT)
> Received: (from sender@localhost)
>   by remote.dom (8.9.3/8.9.3) id NAA20375
>   for user@escom.com; Mon, 6 Sep 1999 21:11:29 -0400 (EDT)
> Date: Mon, 6 Sep 1999 21:11:29 -0400 (EDT)
> From: <sender@remote.dom>
> Message-Id: <199909070111.NAA20375@remote.dom>
> To: user@escom.com
> Subject: example message
>
> This is an example of SMTP message exchange.
> .
< 250 NAA20375 Message accepted for delivery
> quit
< 221 escom.com closing connection

```



Prior Art

Figure 3. Detailed Example of SMTP Message Transfer

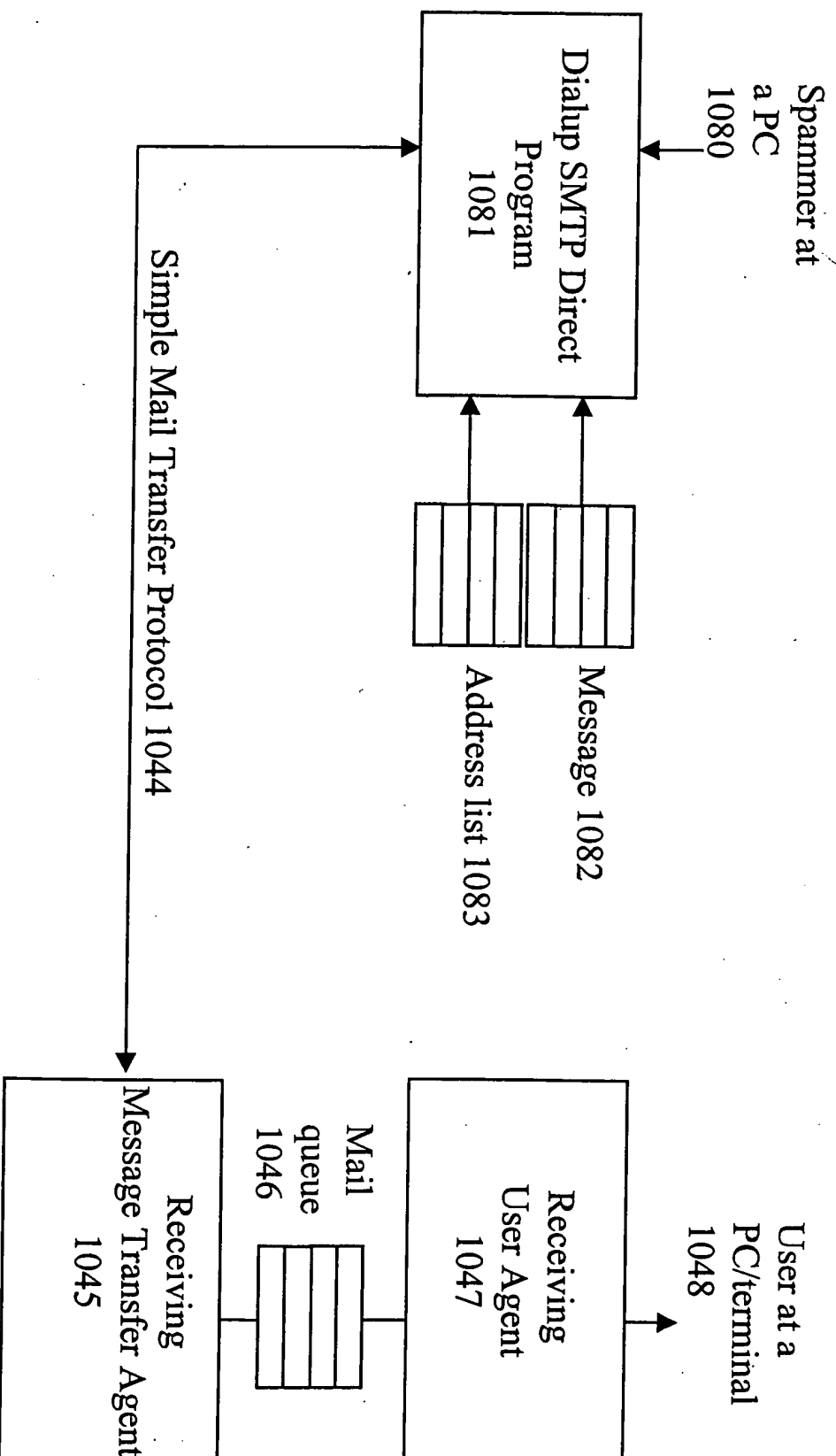
09544322 : 041300


```
< 220 anubis.itesm.dom Sendmail SMI-8.6/SMI-SVR4 ready [...]  
> HELO local.dom  
< 250 anubis.itesm.dom Hello local.dom [...]  
> MAIL From: <relay_test@local.dom>  
< 250 <relay_test@local.dom>... Address ok  
> RCPT To: <nobody@local.dom>  
< 250 <nobody@local.dom>... Recipient ok
```

Prior Art

Figure 5. SMTP Transactions for Relay Test

00549322 : 041200



Prior Art

Figure 6. Dialup SMTP Architecture

FIG. 6. Dialup SMTP Architecture

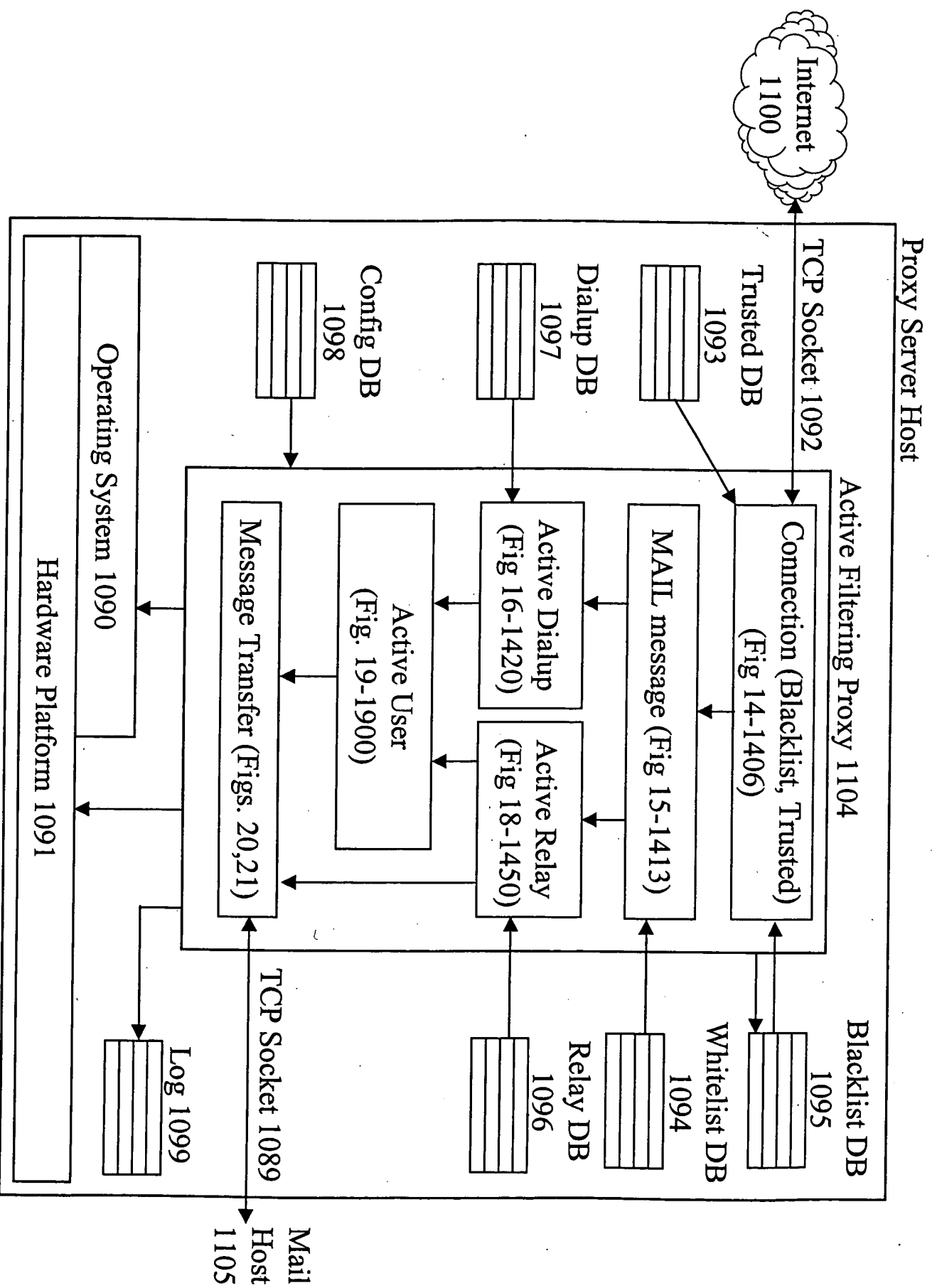


Figure 7 Block Diagram of Active Filtering System

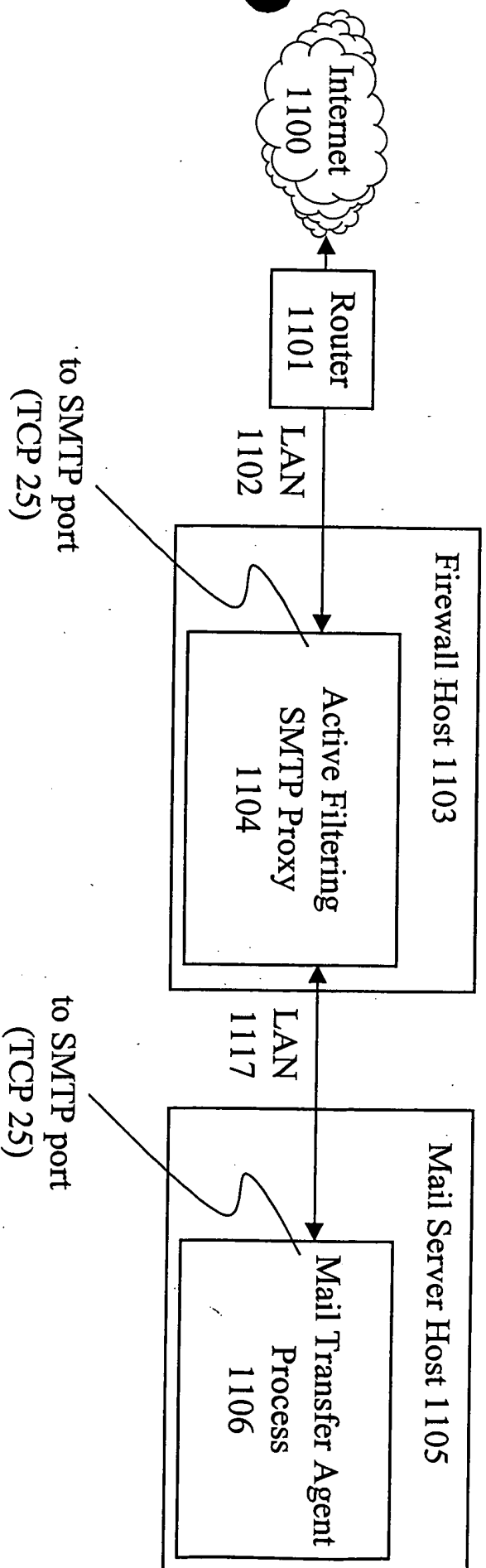


Figure 8. Active Filtering Proxy in Conventional Firewall Configuration.

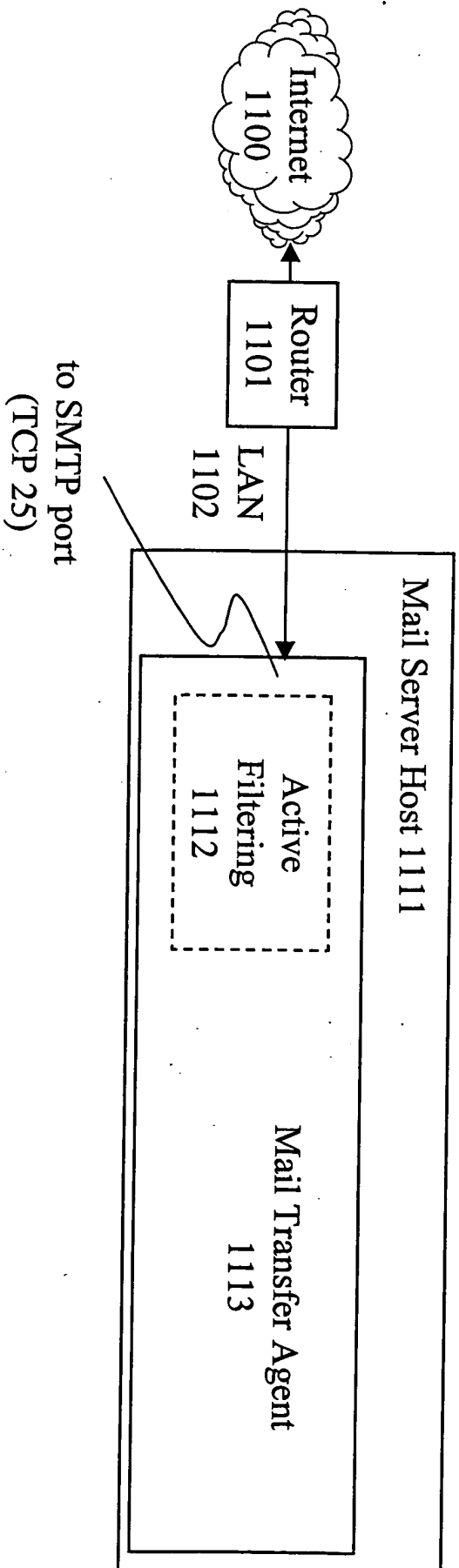


Figure 11. Active Filtering implemented as part of Mail Transfer Agent Process

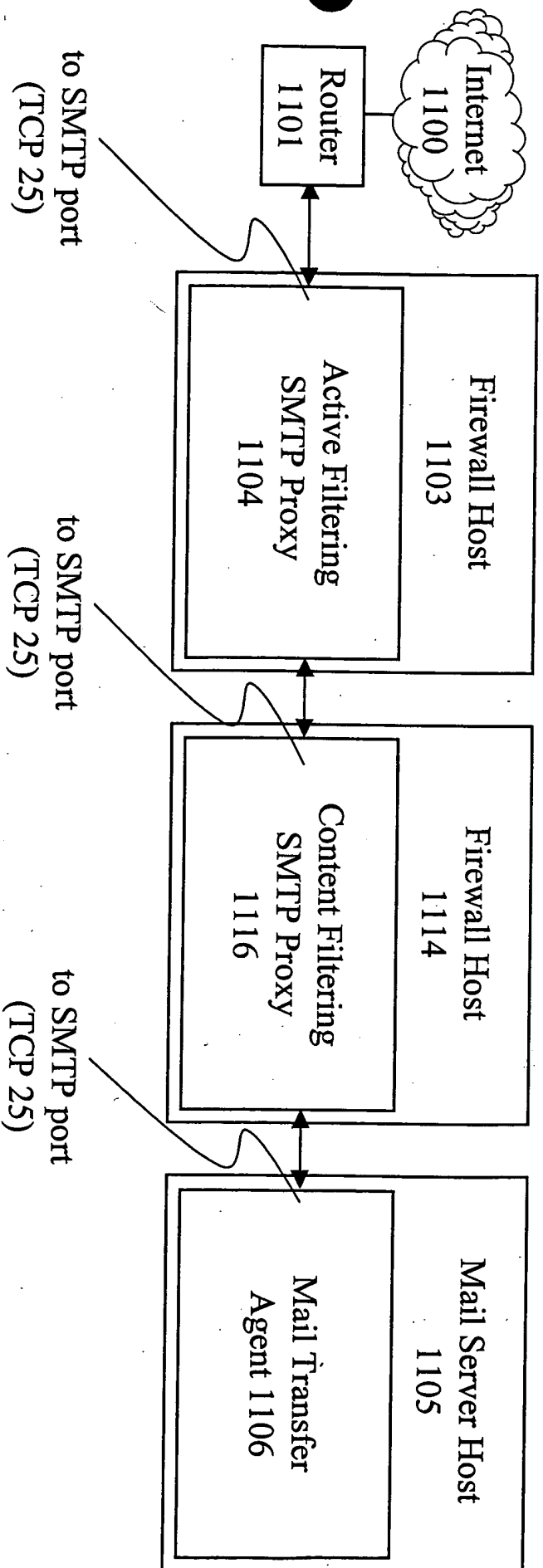


Figure 12. Active Filtering Proxy chained with Content Filtering Proxy

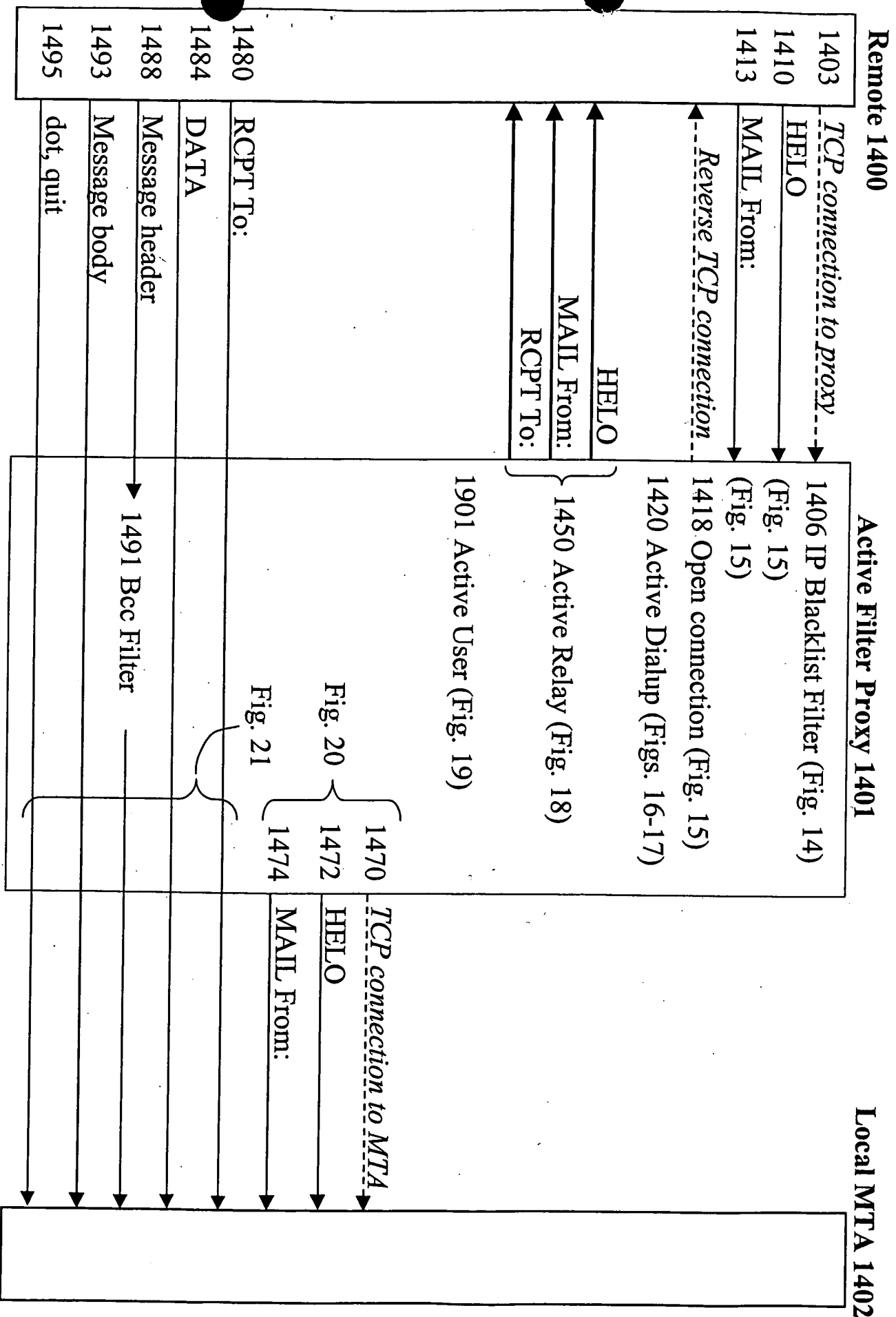


Figure 13. Active Filtering Overview (not showing status responses or error conditions)

Remote 1400

Active Filter Proxy 1401

Local MTA 1402

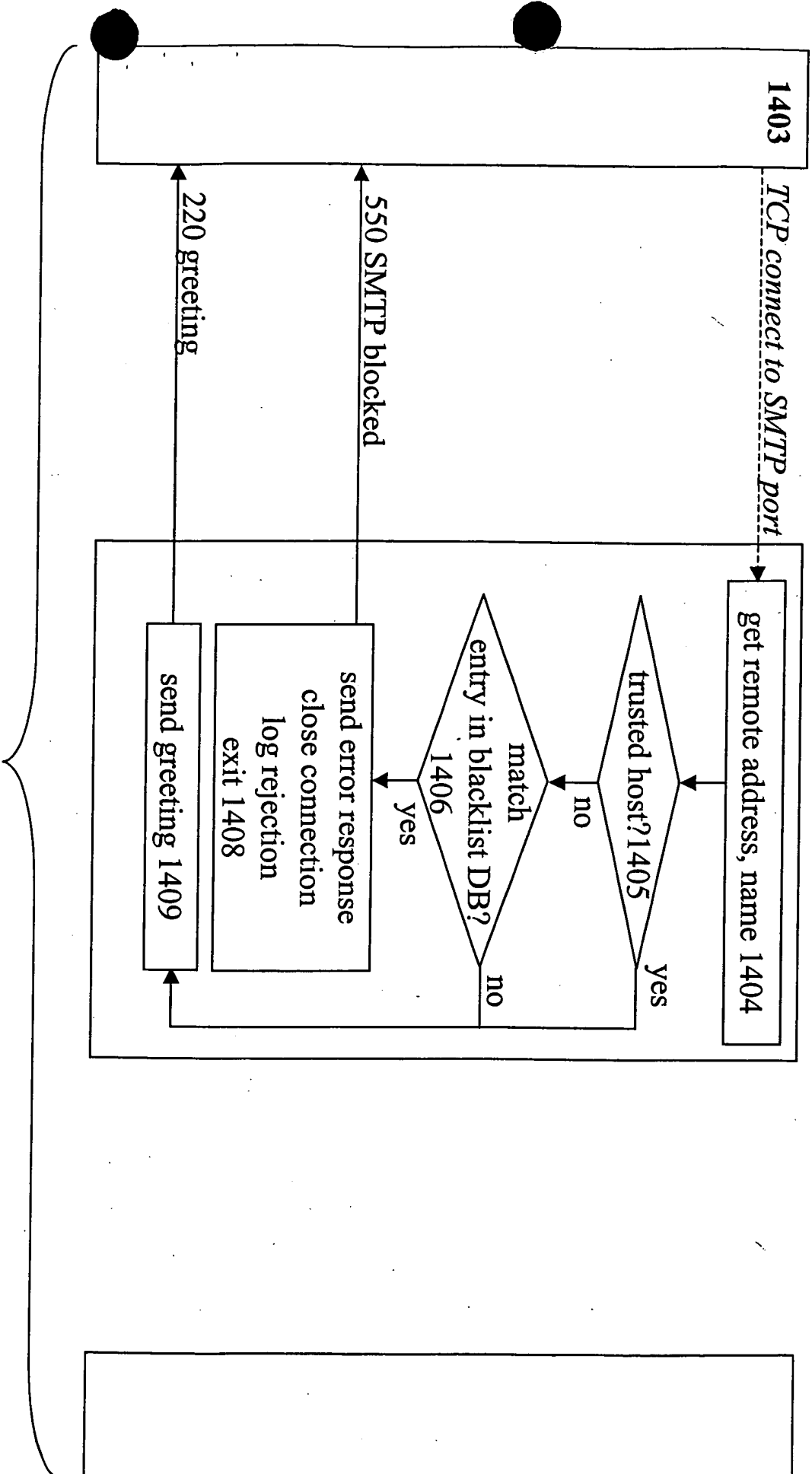


Figure 14. IP Blacklist Filtering

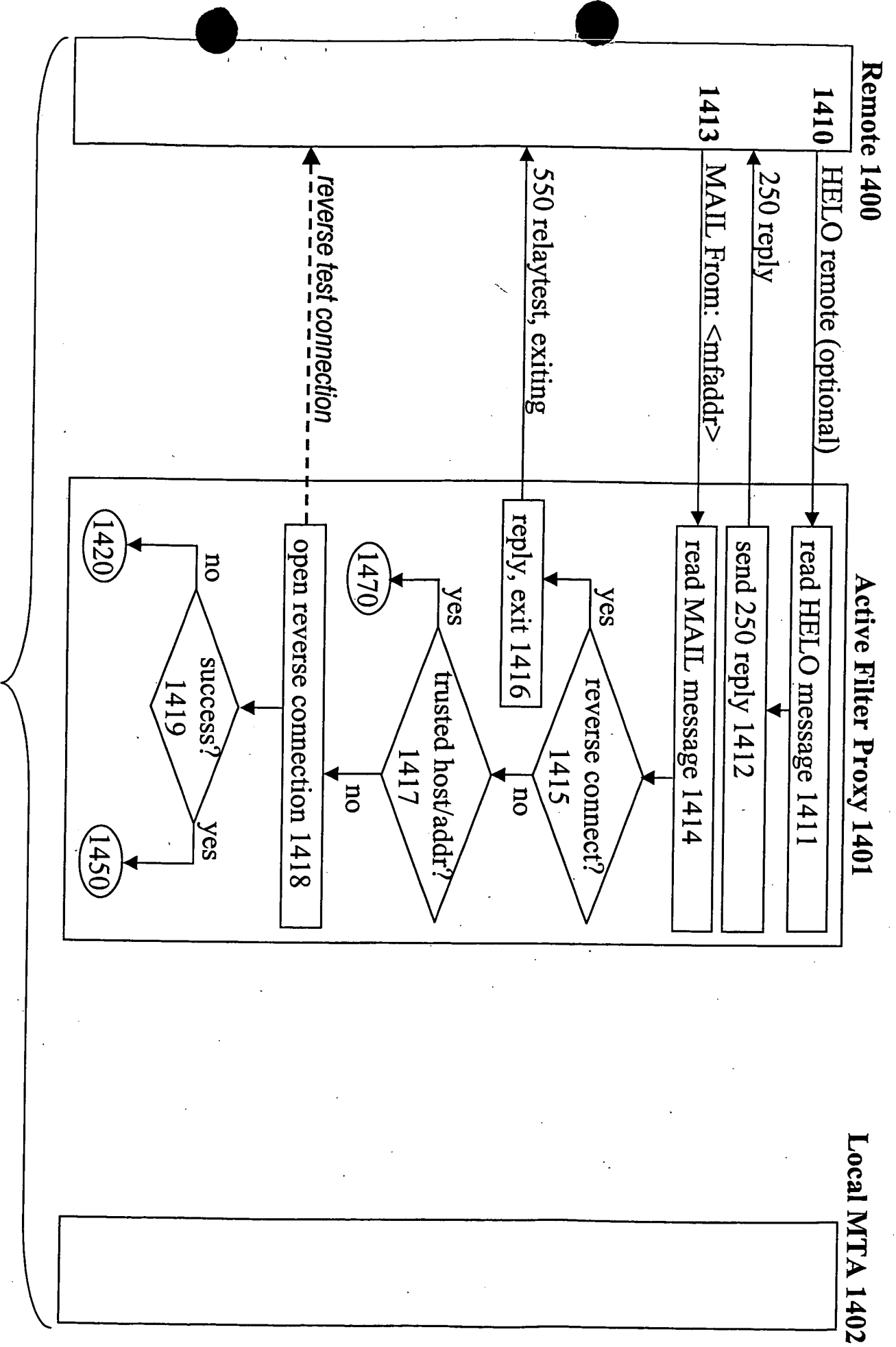
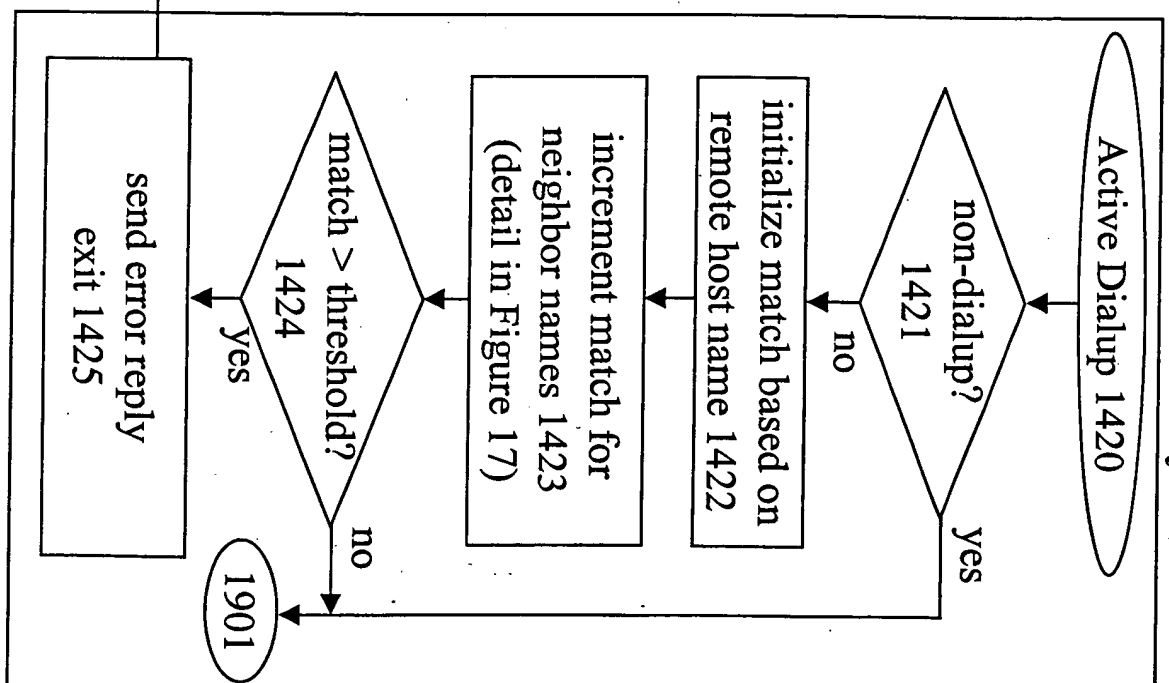


Figure 15. Remote HELLO and MAIL Message Processing

Remote 1400

Active Filter Proxy 1401

Local MTA 1402



550 Apparent dialup

Figure 16. Active Dialup Test

Remote 1400

Active Filter Proxy 1401

Local MTA 1402

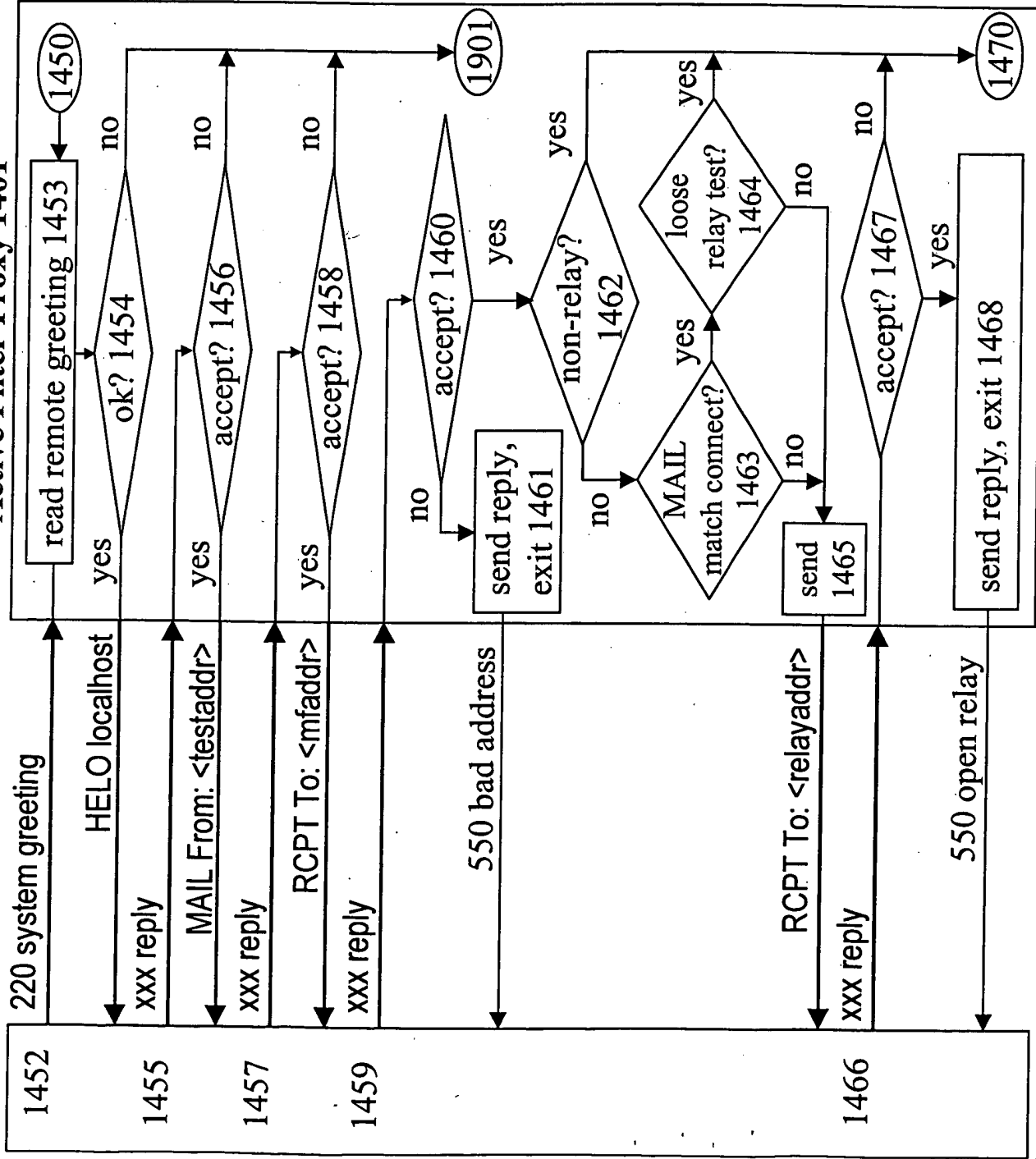


Figure 18: Active Relay Test

Mailhost 1900

Active Filter Proxy 1401

Local MTA 1402

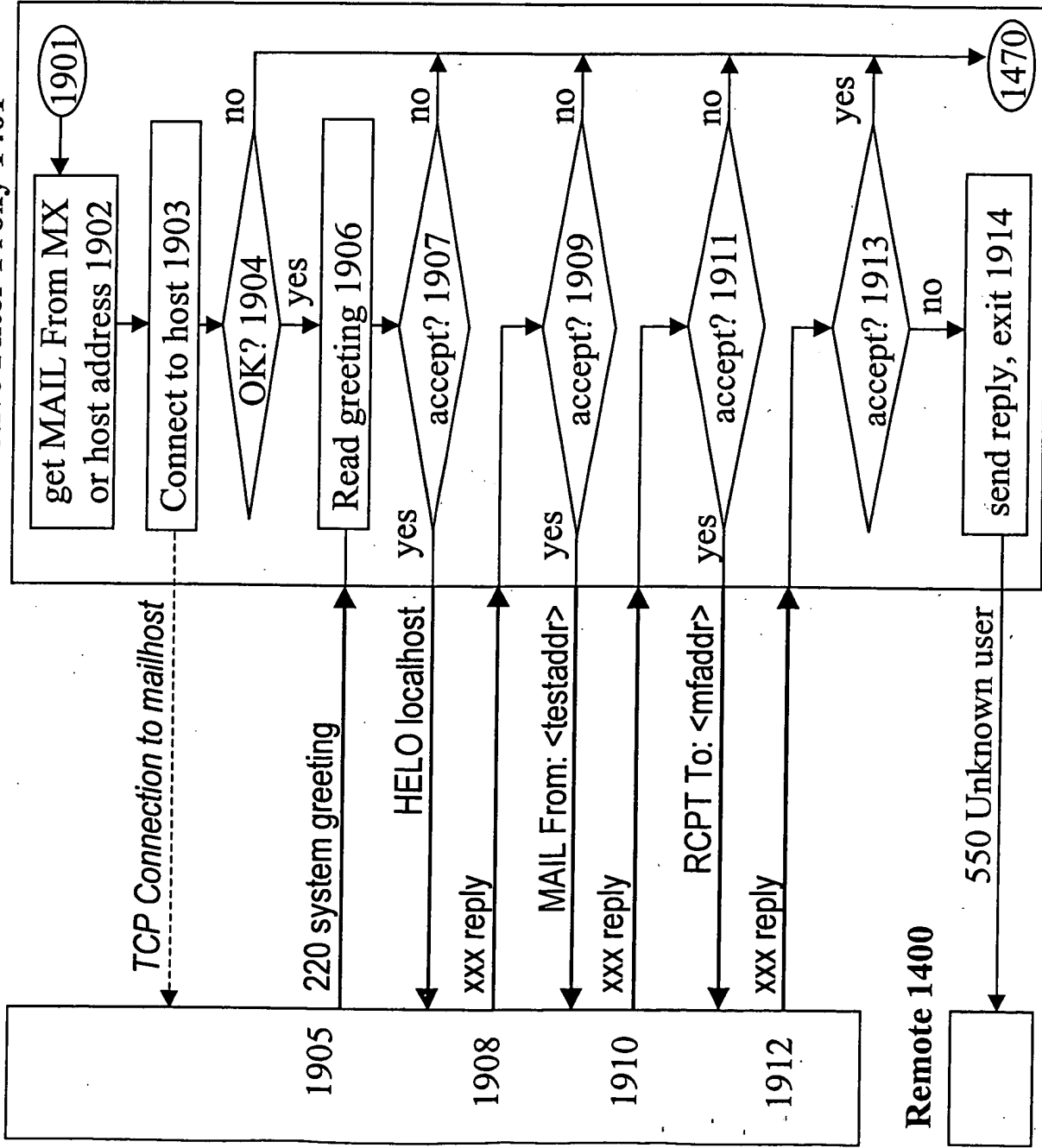


Figure 19. Active User Test

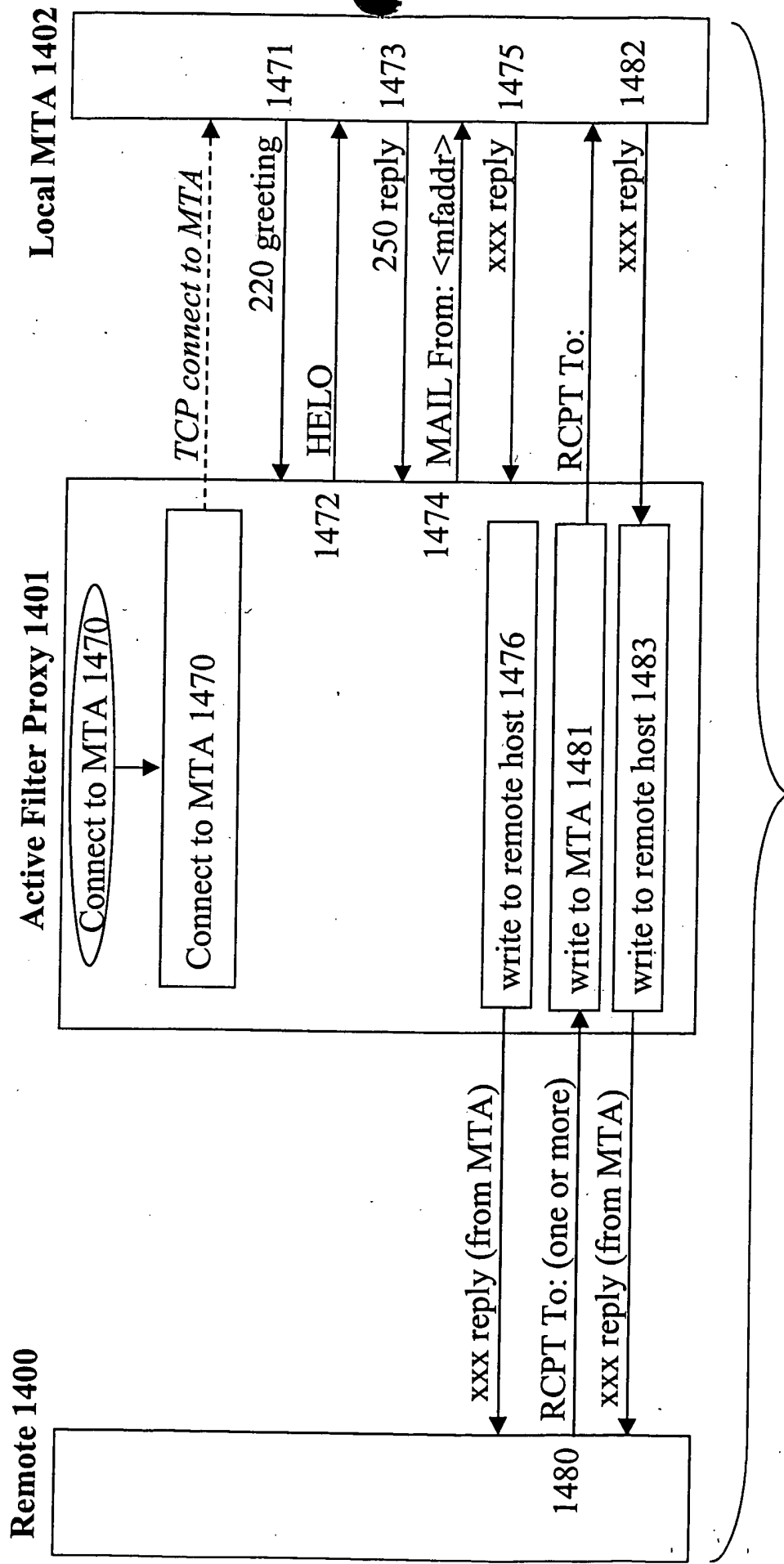


Figure 20. Connect to MTA and Early Protocol Messages

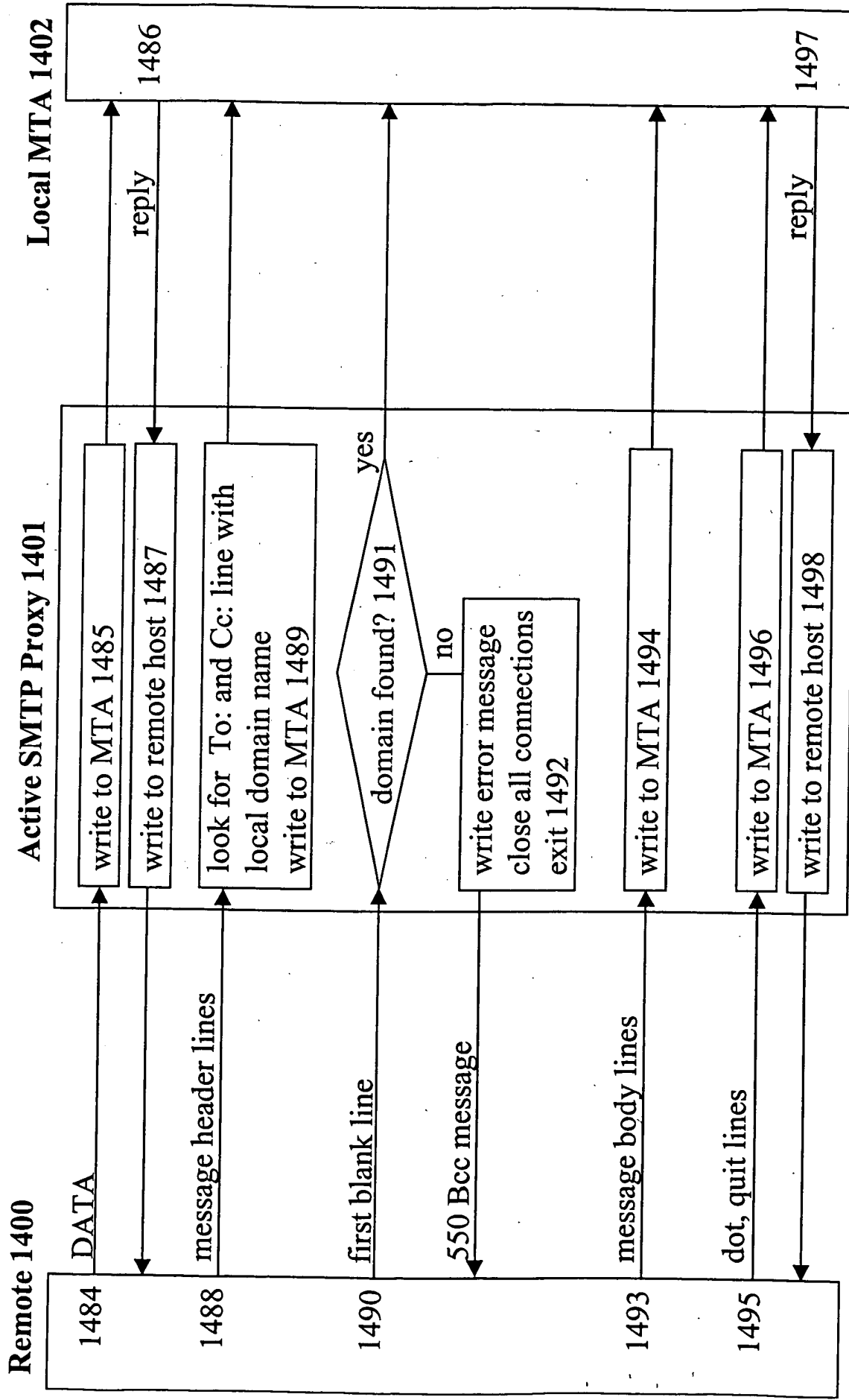


Figure 21. Data Transfer Phase

00000000000000000000000000000000

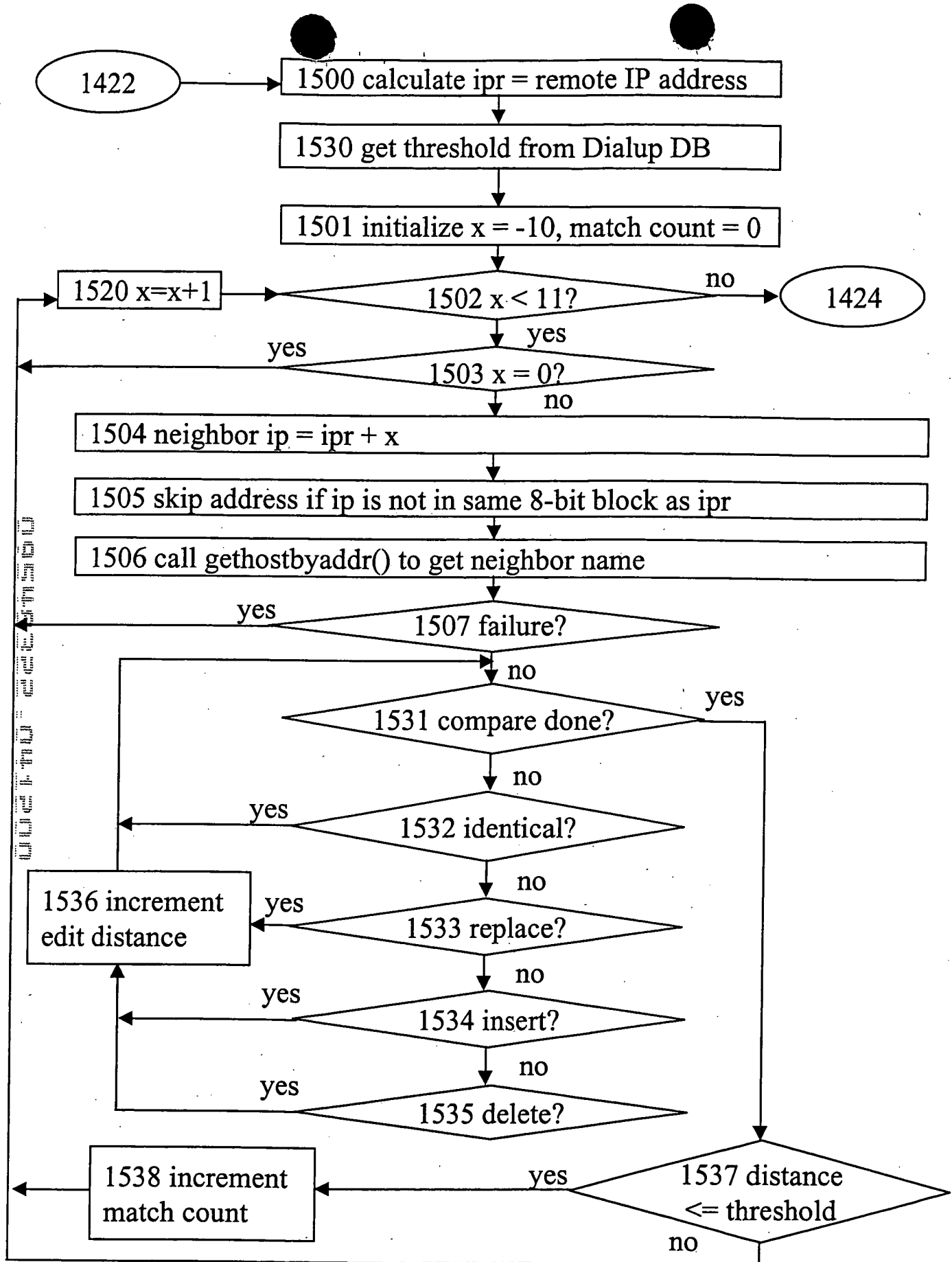


Figure 22. Details of Edit Distance Method
(Alternative Figure 16 Step 1423)

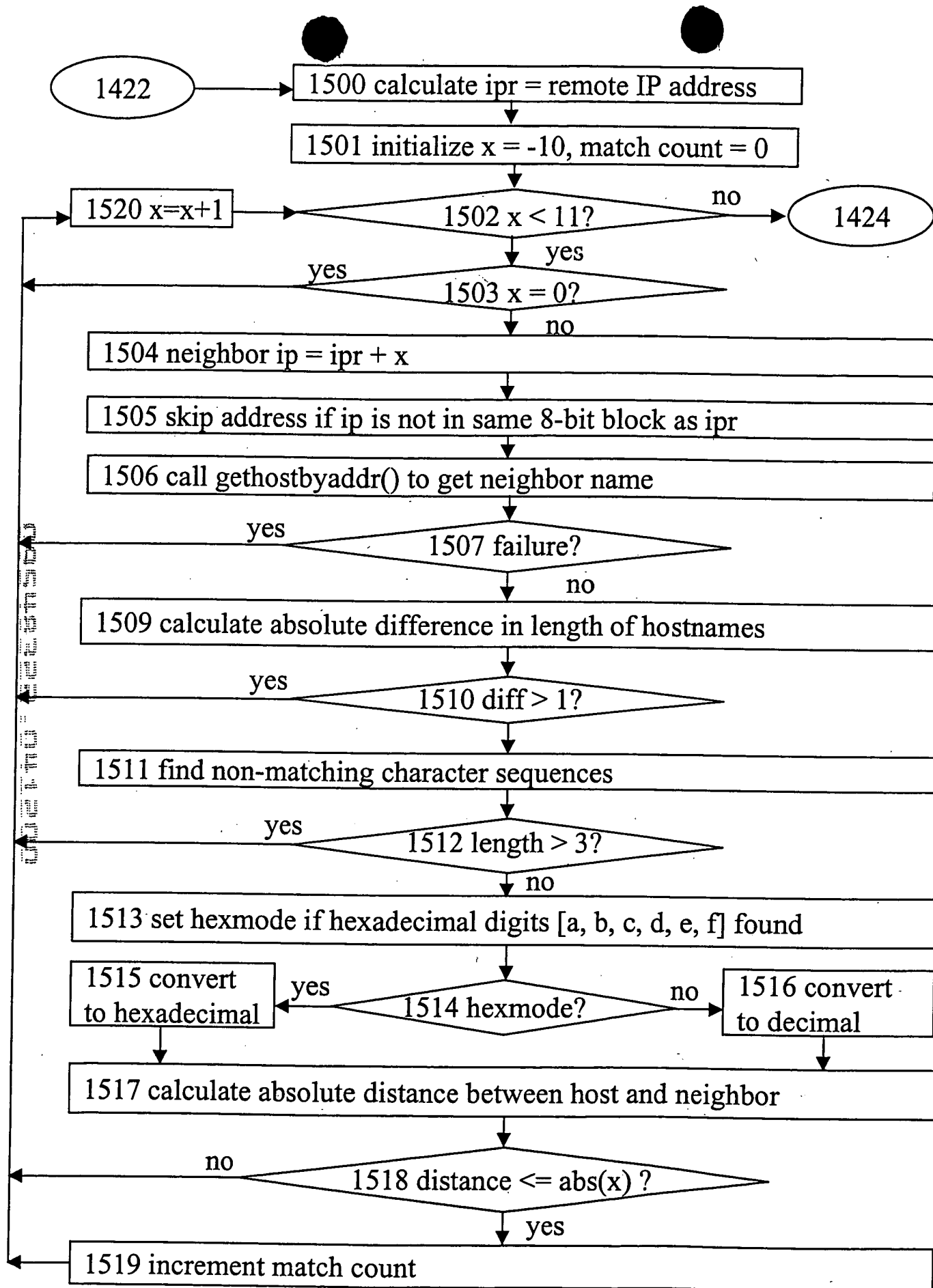


Figure 17. Details of Figure 16 Step 1423

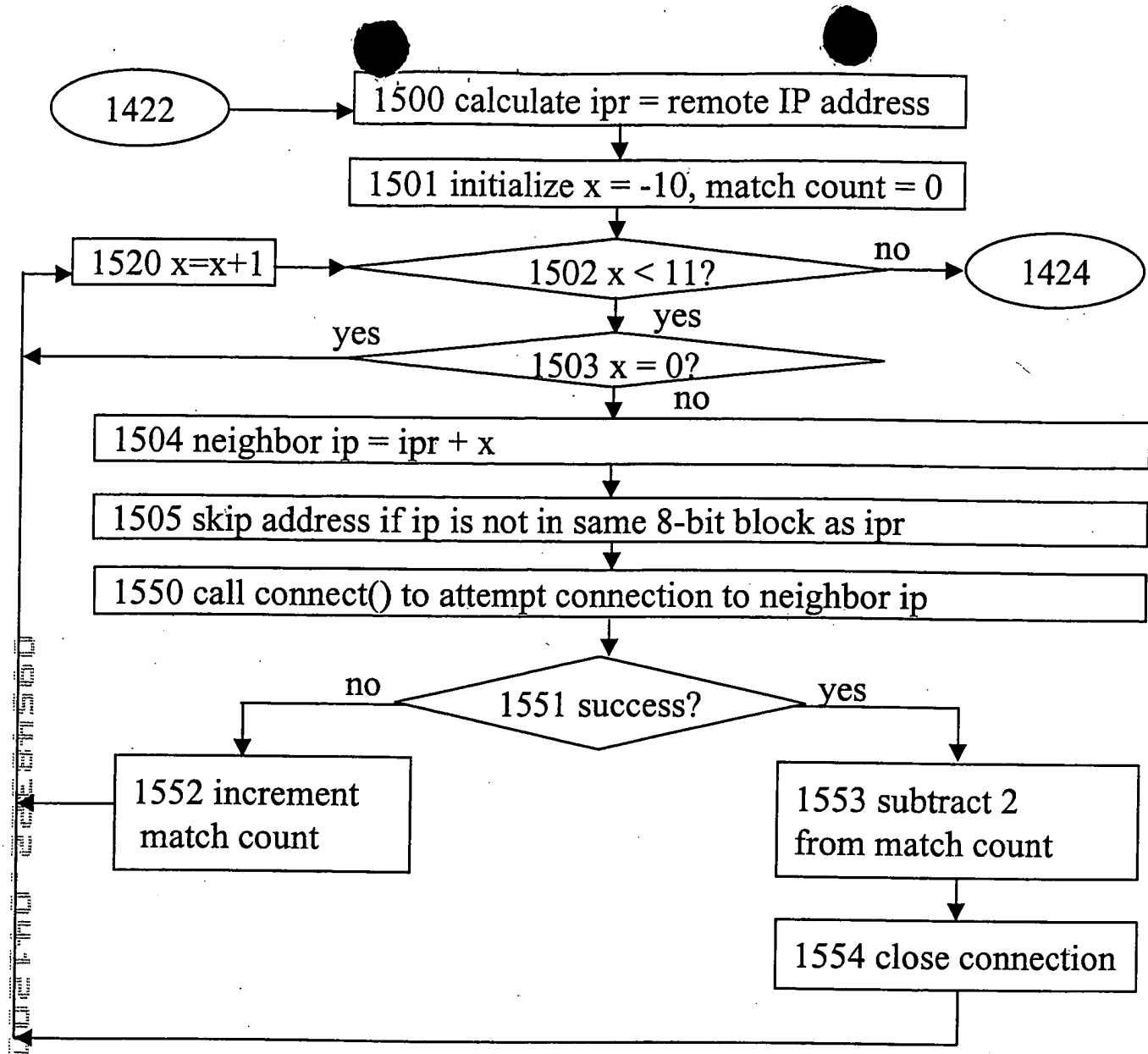


Figure 23. Details of Neighbor Connection Method
(Alternative Figure 16 Step 1423)

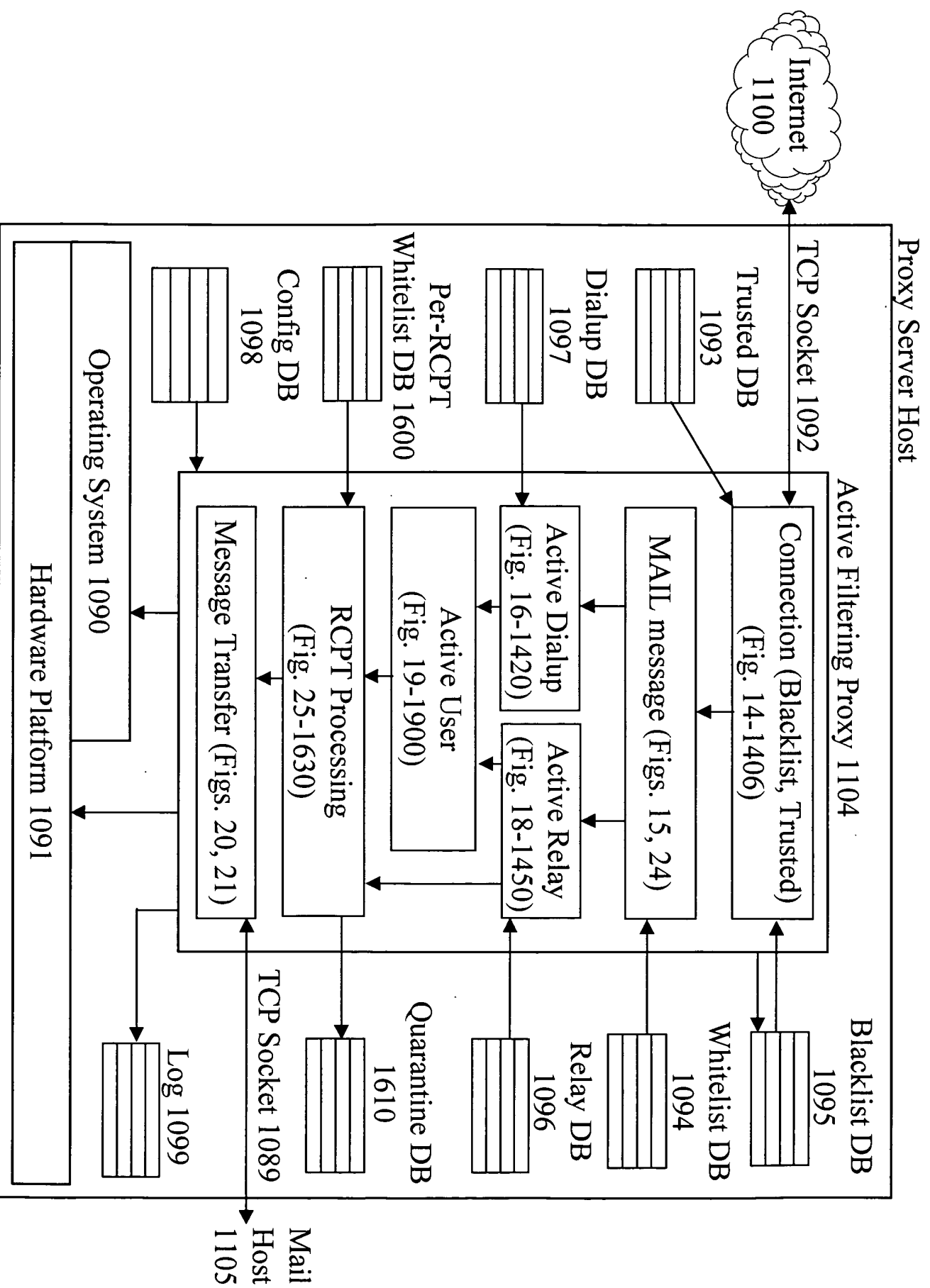


Figure 24. Active Filtering with Per-Recipient Whitelists and Quarantining.

Remote 1400

Active Filter Proxy 1401

Local MTA 1402

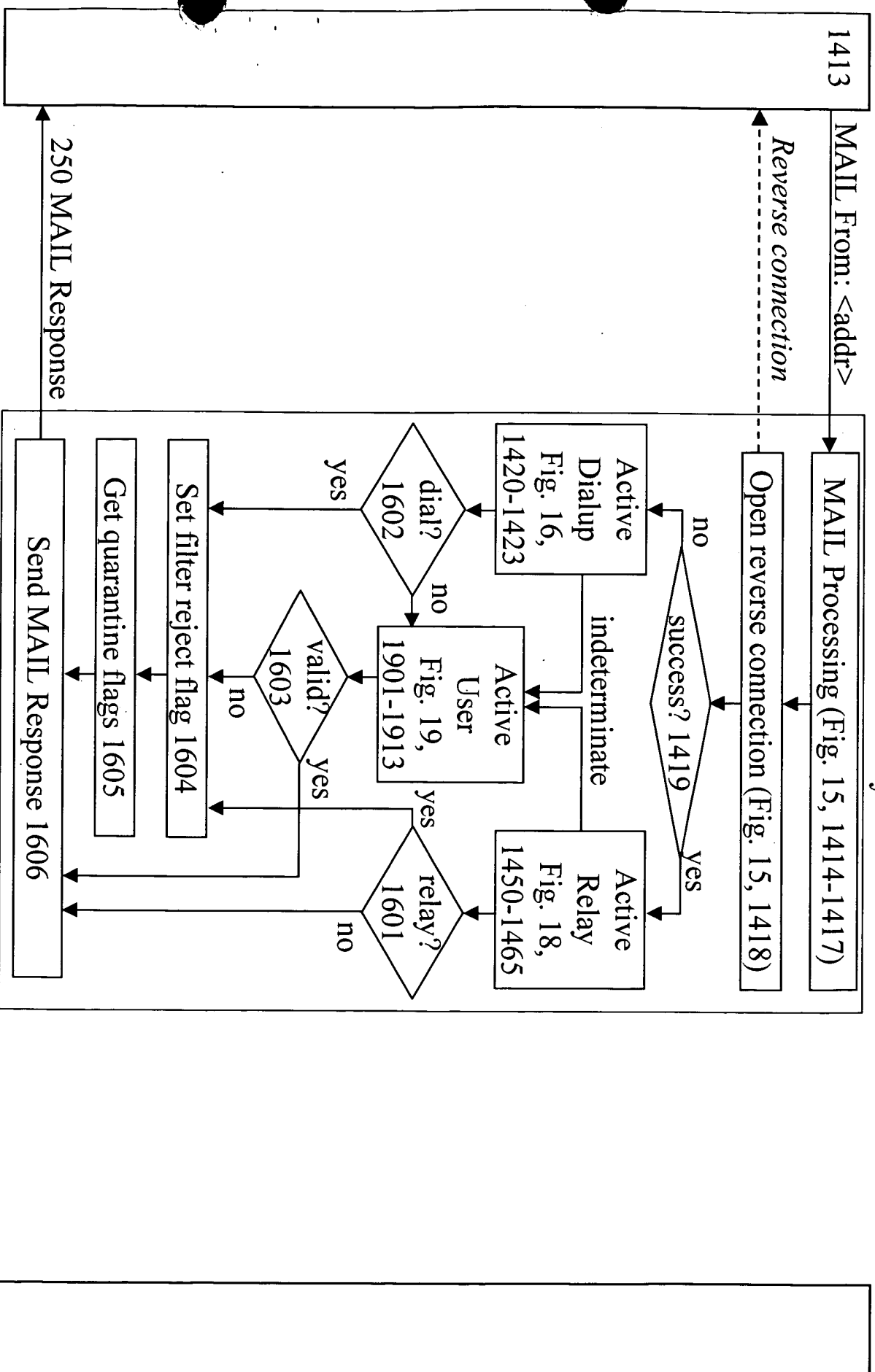


Figure 25. MAIL Processing.

Remote 1400

Active Filter Proxy 1401

Local MTA 1402

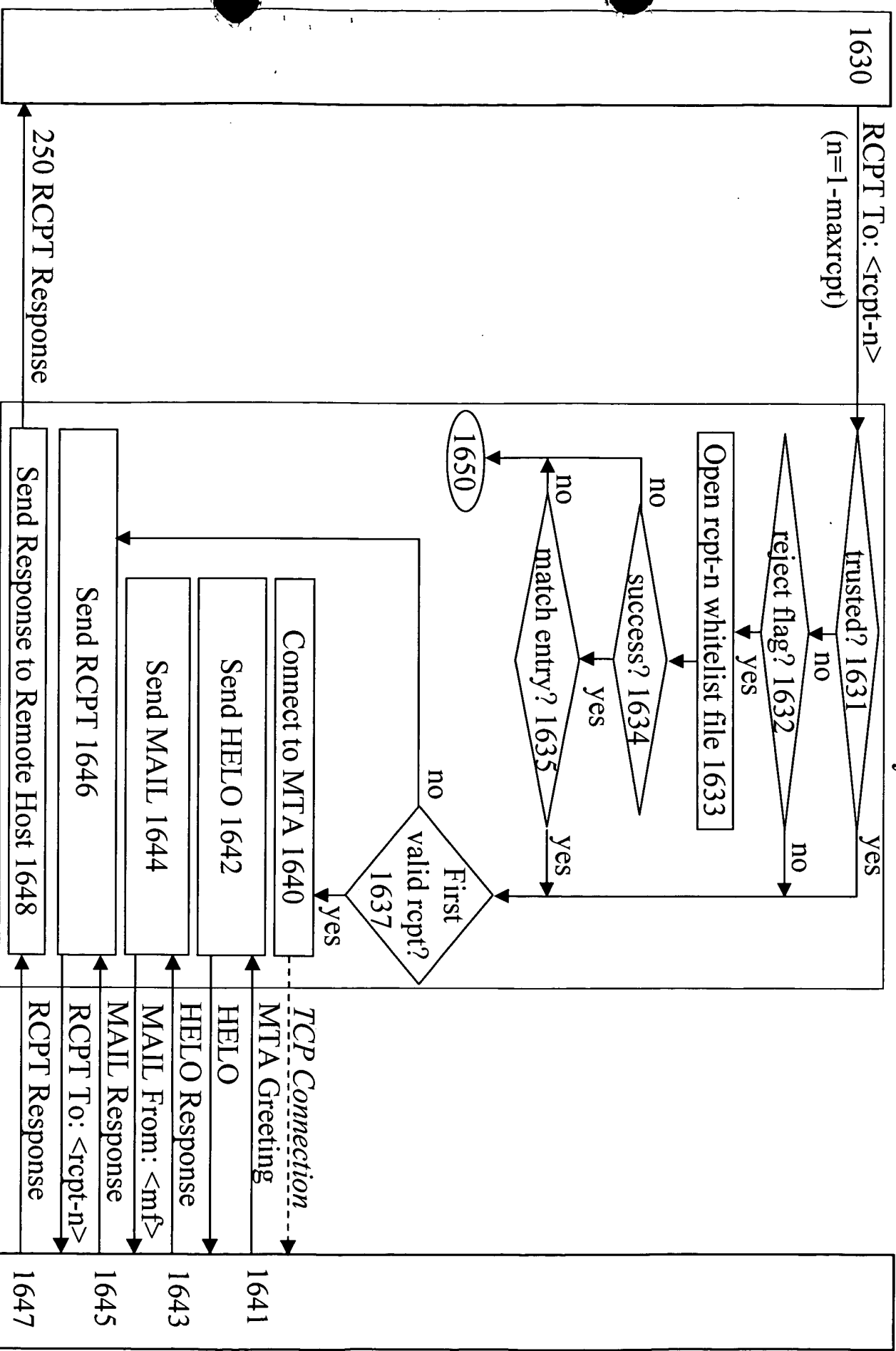


Figure 26 Per-RCPT Whitelist Processing

Remote 1400

Active Filter Proxy 1401

Local MTA 1402

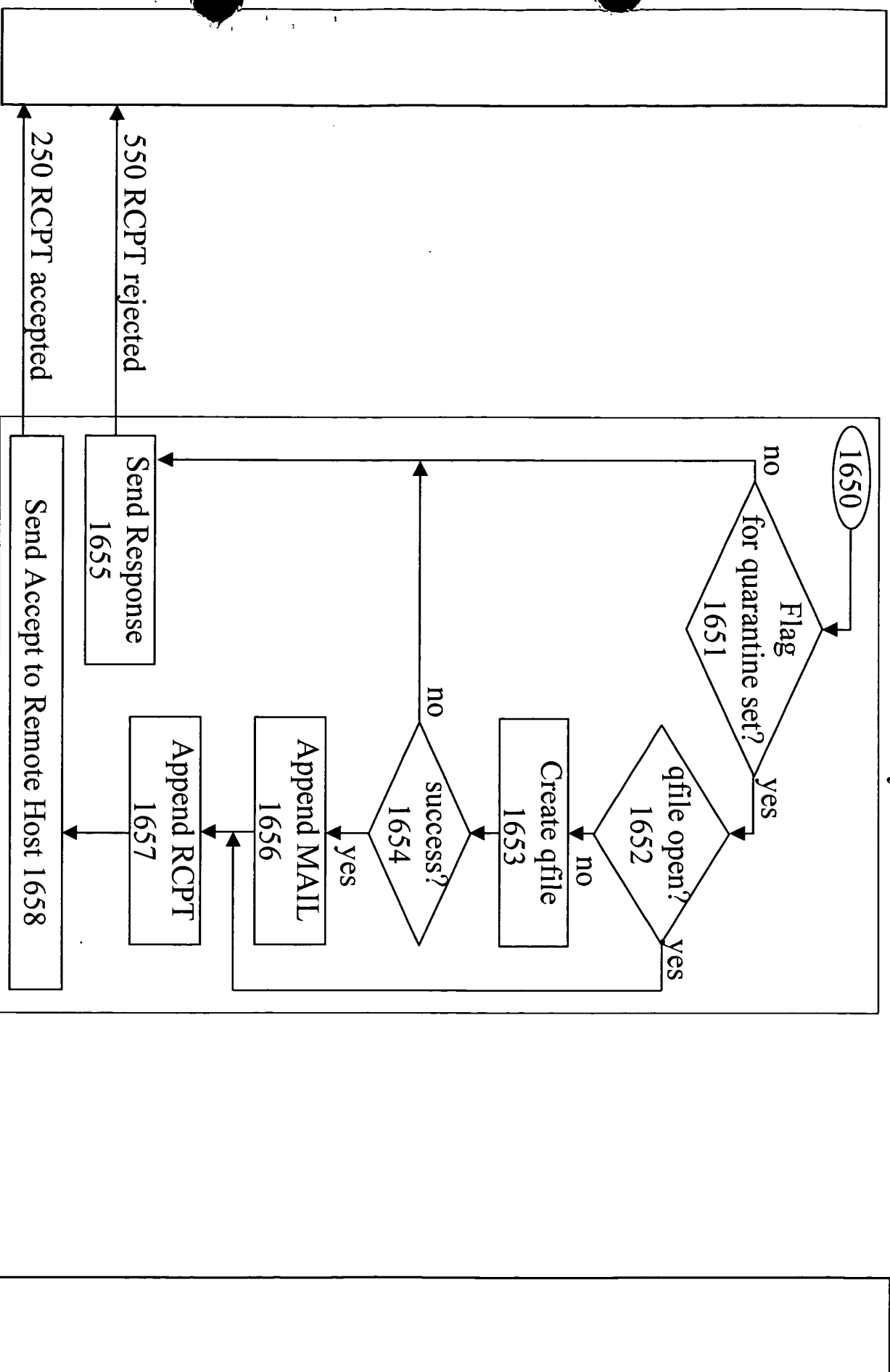


Figure 27 RCPPT Quarantine Processing.

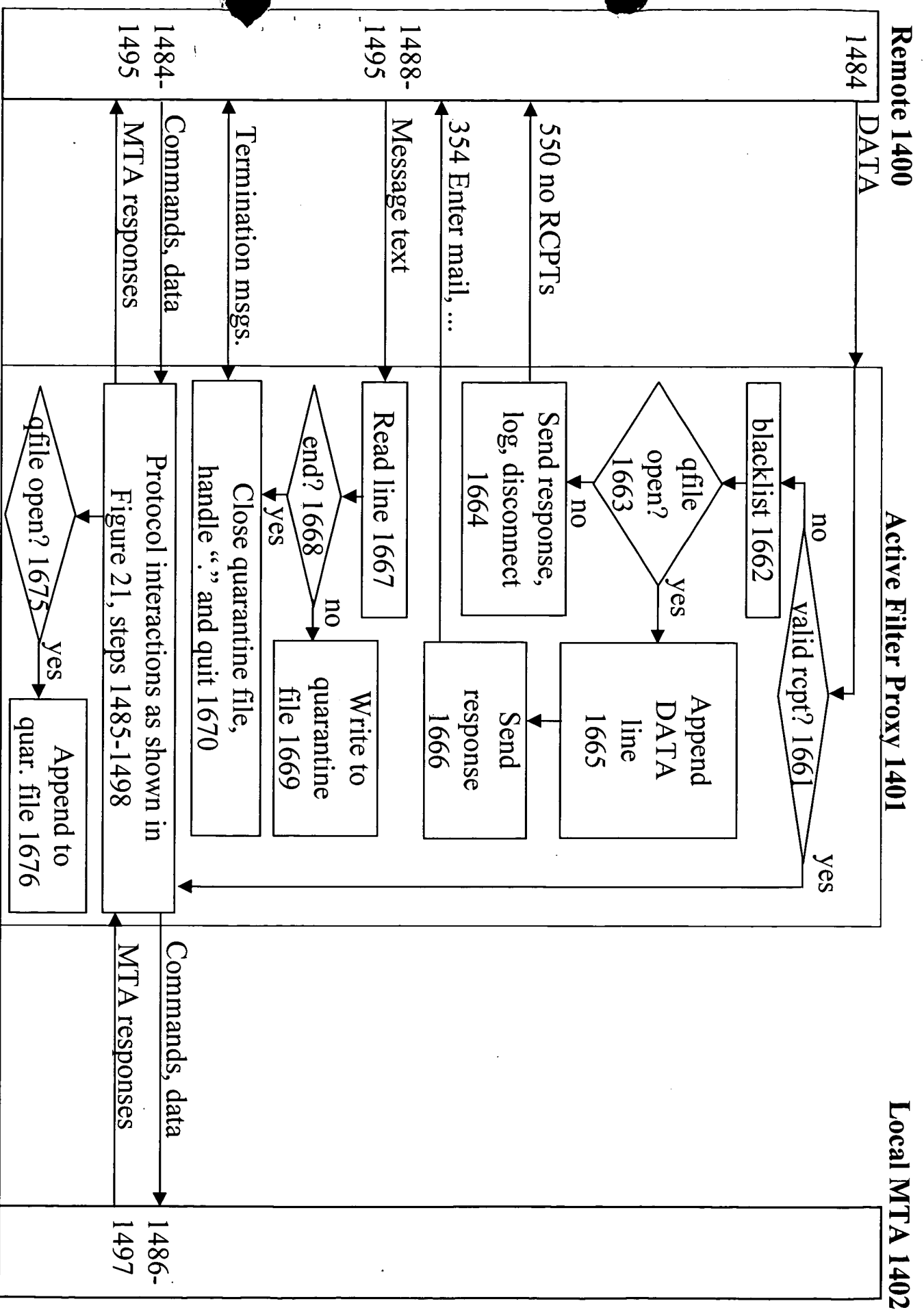


Figure 28 DATA and Message Text Processing.

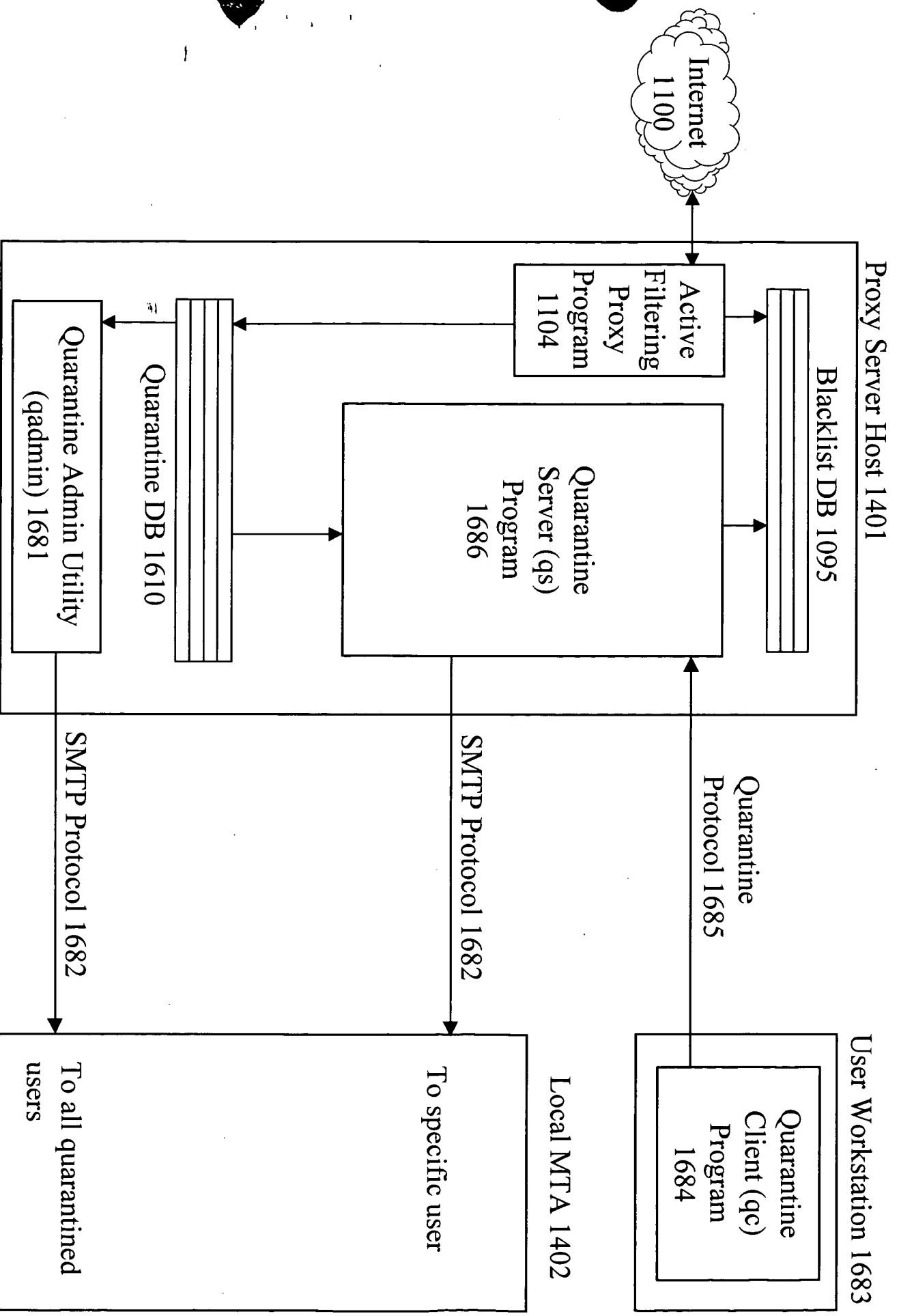


Figure 29. Quarantined Message Retrieval